Multisignature - Uživatelská příručka

MathAn Praha, s.r.o.

Obsah

Kapitola 1. Aplikace pro vícenásobný elektronický podpis

Aplikace Multisignature slouží k vytváření elektronických podpisů několika podpisujícími stranami a k ověřování jejich platnosti. Vytvořené vícenásobné podpisy sestávají z běžných elektronických podpisů, jež jsou podpisy dle zákona č. 227/2000 Sb., o elektronickém podpisu.

Aplikace nabízí následující základní funkčnosti:

- Podpis dokumentu několika podepisujícími stranami;
- Management klíčů a certifikátů;
- Zahájení procesu podepisování;
- Podepsání dokumentu jedním podpisovatelem - dílčí podpis;
- Spojení souborů s dílčími podpisy do jednoho souboru;
- Uzavírací podpis a vytvoření uzavřeného vícenásobně podepsaného dokumentu;
- Potvrzení doručenky;
- Vytvoření uzavřeného vícenásobně podepsaného dokumentu s doručenkami;
- Ověření platnosti podpisů ve vícenásobně podepsaném dokumentu.

Kapitola 2. Základní principy a funkce aplikace

- Podpisované dokumenty jsou v binární podobě vloženy do XML souboru (XML obálky) a jsou k nim přiloženy i pokyny pro podpisující strany. Všechny podpisy jsou realizovány s použitím formátu XML Signature (formát XAdES dle normy ETSI TS 101 903) a vloženy do XML obálky k podpisovaným dokumentům.

- Aplikace je vytvořena v programovacím jazyce Java a tím je umožněno její použití na všech platformách (operačních systémech), kde je běhové prostředí Java implementováno. Jsou to prakticky všechny běžně používané platformy: MS Windows, Linux i jiné varianty Unixu, u platformy MacOS X bohužel zatím není potřebná verze Javy implementována.

- Aplikace se spouští z webu, avšak běží na klientském počítači. Prostředek pro spouštění je technologie Java Web Start, která zajišťuje transparentní aktualizaci aplikace před každým jejím spuštěním.

- Podpisy nejsou opatřovány časovým razítkem, ale nabízí se možnost vložení podepsaného atributu obsahujícího čas. Také existuje možnost vložení uzavíracího podpisu (kontrasignatury), který podepíše všechny dříve vložené podpisy.

Kapitola 3. První spuštění aplikace

Aplikace Multisignature nevyžaduje žádnou instalaci.Pro běh je nutné mít nainstalované běhové prostředí jazyka Java (JRE – Java Runtime Environment) ve verzi 6.0. To zdarma získáte ze stránek www.java.com. Vyberte si instalaci pro svůj operační systém. Pro uživatele MS Windows je výhodnější zvolit režim instalace off-line.

K prvnímu spuštění aplikace je potřeba vykonat následující kroky. Máte-li běhové prostředí Java již nainstalované, krok 1 přeskočte.

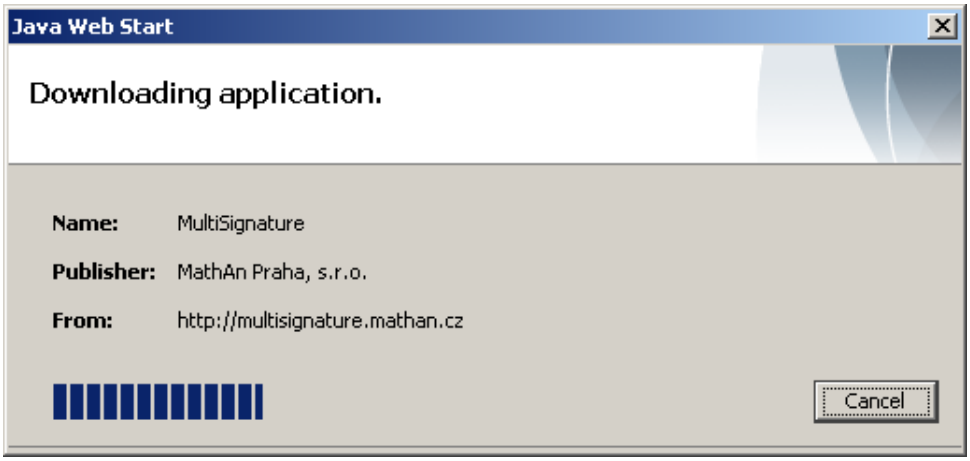
1. Získat běhové prostředí Java [http://www.java.com/en/download/manual.jsp], nainstalovat je, a posléze webový prohlížeč ukončit a znovu spustit.

2. Tímto odkazem spustit aplikaci [http://multisignature.mathan.cz/jws/jnlp/multisignature-normal.jnlp].

Při spuštění aplikace prohlížeč nejprve získá řídící soubor typu JNLP. Možná jej nabídne k uložení, avšak je třeba prohlížeč přimět, aby tento soubor otevřel pomocí programu javaws (Java Web Start), který je součástí instalace běhového prostředí jazyka *Java*. Pokud se možnost otevření programem *javaws* nenabízí, je třeba zopakovat instalaci běhového prostředí jazyka *Java verze 6.0* a vypnutí a opětovné spuštění webového prohlížeče.

Pokud spuštění proběhlo v pořádku, objeví se pomocné informativní okno s nápisem *Java™ Starting...*

Poté se objeví okno informující o průběhu stahování souborů potřebných pro běh aplikace. Při opakovaném spuštění aplikace se nejprve ověří, zda je stažená verze aktuální, a ze serveru se stáhnou pouze soubory, které byly od posledního spuštění aplikace aktualizovány. Při dalších spuštěních se typicky zjistí, že není třeba nic aktualizovat, a toto ověření proběhne rychle. Při prvním spuštění se však musí získat celý kód aplikace včetně knihoven, což představuje přibližně 4 megabajty.



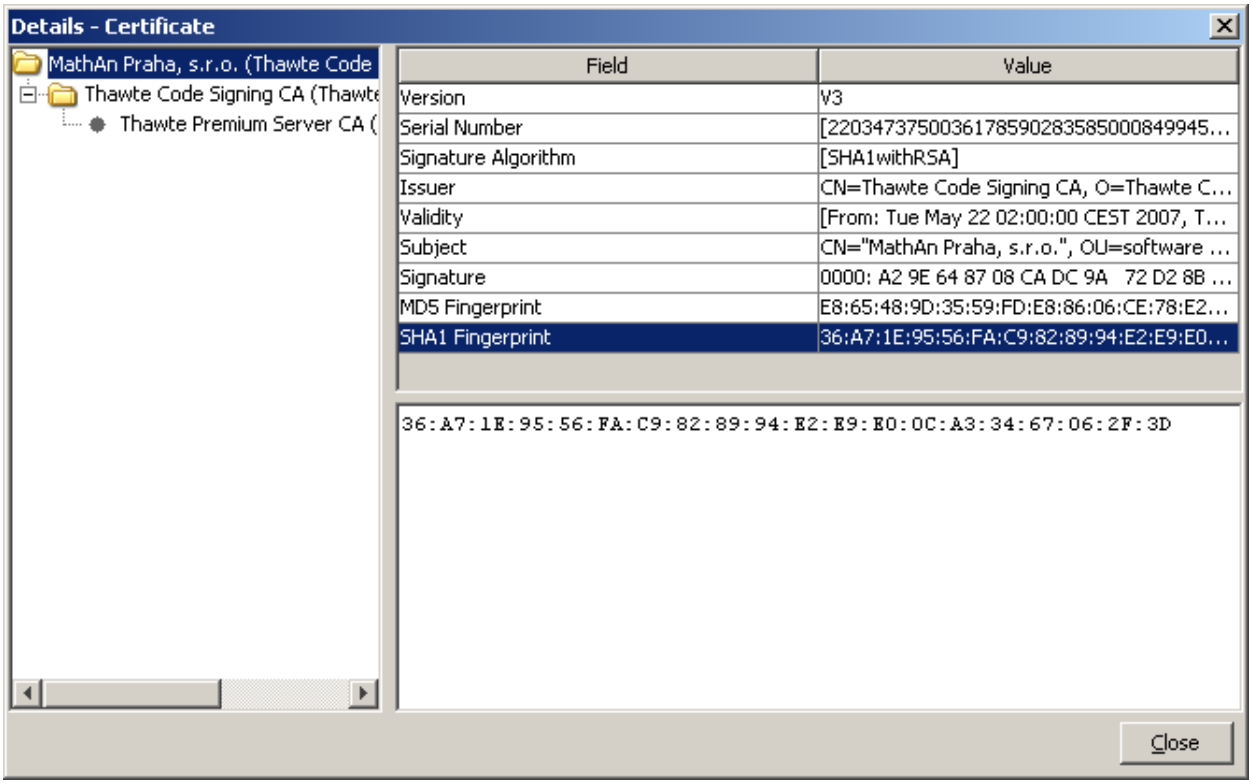
Po stažení všech souborů aplikace proběhne ověření podpisu aplikace. Je důležité, abyste zkontrolovali následující:

- Aplikace se jmenuje **Multisignature**
- Aplikace je podepsána certifikátem vydaným společnosti **MathAn Praha, s.r.o.**

Odkaz *More Information...* by měl zobrazit následující informace, které neobsahují žádná varování:

- Tato aplikace bude spuštěna bez bezpečnostních omezení, která obvykle běhové prostředí Java poskytuje
- Pozor,"MathAn Praha s.r.o." prohlašuje, že aplikace je bezpečná. Spusťte tuto aplikaci pouze v případě, že "MathAn Praha s.r.o." věříte toto tvrzení.
- Digitální podpis byl vytvořen důvěryhodným certifikátem

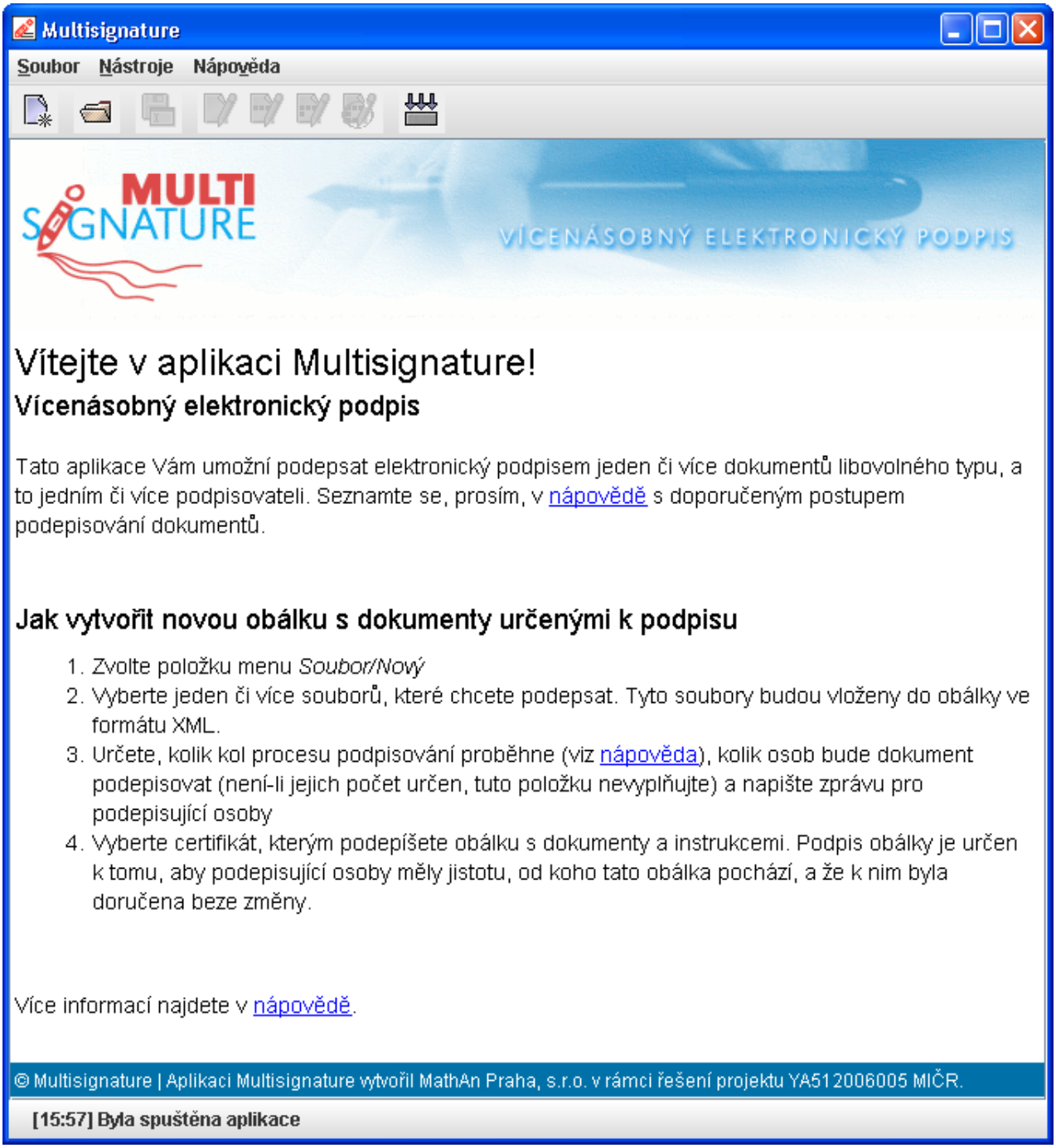
Kliknutím na odkaz *Certificate details...* zobrazíte podrobnosti certifikátu, kterým je aplikace podepsána:



Zde byste měli ověřit, že se jedná o certifikát určený pro podpis kódu, vydaný společností Thawte Consulting cc [http://www.thawte.com/], jedním z významných certifikačních úřadů světa.

Pokud vše souhlasí, tlačítkem *Run* dáte souhlas ke spuštění aplikace.

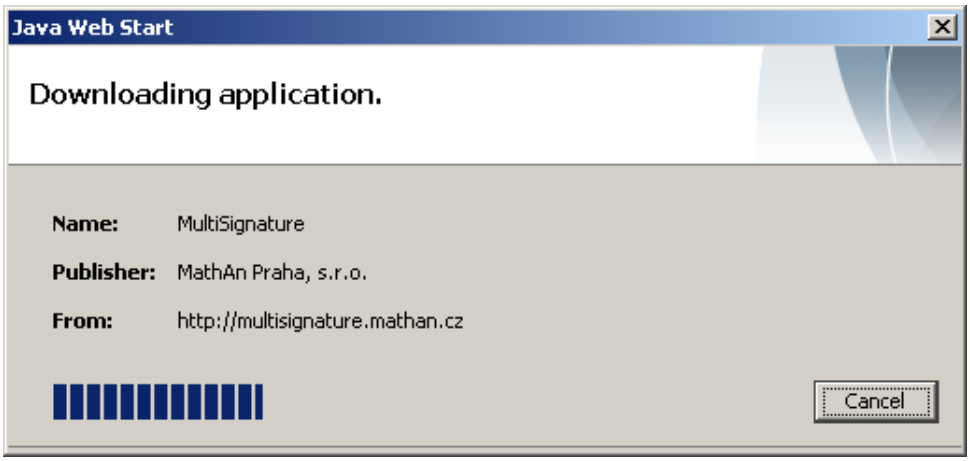
Aplikace po krátké inicializaci zobrazí svou základní obrazovku:


Multisignature
Soubor Nástroje Nápověda
MULTI SIGNATURE
VÍCENÁSOBNÝ ELEKTRONICKÝ PODPIS
Vítejte v aplikaci Multisignature!
Vícenásobný elektronický podpis
Tato aplikace Vám umožní podepsat elektronický podpisem jeden či více dokumentů libovolného typu, a to jedním či více podpisovateli. Seznamte se, prosím, v nápovědě s doporučeným postupem podepisování dokumentů.
Jak vytvořit novou obálku s dokumenty určenými k podpisu
1. Zvolte položku menu Soubor/Nový
2. Vyberte jeden či více souborů, které chcete podepsat. Tyto soubory budou vloženy do obálky ve formátu XML.
3. Určete, kolik kol procesu podpisování proběhne (viz nápověda), kolik osob bude dokument podepisovat (není-li jejich počet určen, tuto položku nevyplňujte) a napište zprávu pro podepisující osoby
4. Vyberte certifikát, kterým podepíšete obálku s dokumenty a instrukcemi. Podpis obálky je určen k tomu, aby podepisující osoby měly jistotu, od koho tato obálka pochází, a že k nim byla doručena beze změny.
Více informací najdete v nápovědě.
© Multisignature | Aplikaci Multisignature vytvořil MathAn Praha, s.r.o. v rámci řešení projektu YA512006005 MIČR.
[15:57] Byla spuštěna aplikace

Kapitola 4. Další spuštění aplikace

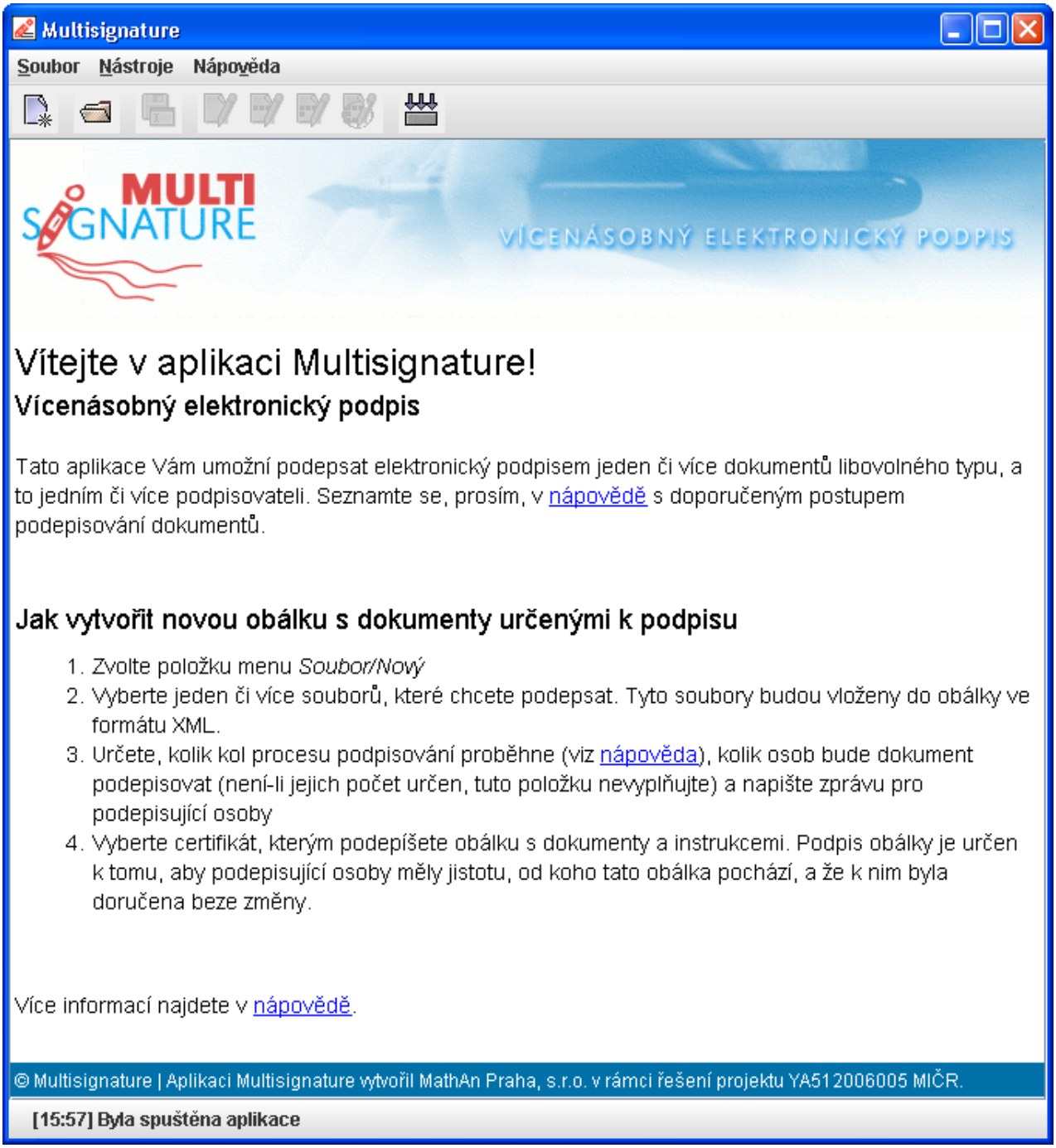
Aplikace se vždy spouští s použitím odkazu http://multisignature.mathan.cz/jws/jnlp/multisignature-normal.jnlp. Pokud spuštění proběhlo v pořádku, objeví se pomocné informativní okno s nápisem *Java™ Starting...*

Při opakovaném spuštění aplikace se nejprve ověří, zda je stažená verze aktuální, a ze serveru se stáhnou pouze soubory, které byly od posledního spuštění aplikace aktualizovány. Je-li potřeba nějaké soubory stáhnout, objeví se okno informující o průběhu jejich aktualizace.



Při dalších spuštěních se typicky zjistí, že není třeba nic aktualizovat, a tedy se výše uvedené okno nezobrazí. Nezobrazují se ani informace o podpisu aplikace, neboť ověření podpisu se provádí pouze při prvním spuštění aplikace.

Po krátké inicializaci se zobrazí hlavní okno aplikace Multisignature.


Multisignature
Soubor Nástroje Nápověda
MULTI SIGNATURE
VÍCENÁSOBNÝ ELEKTRONICKÝ PODPIS
Vítejte v aplikaci Multisignature!
Vícenásobný elektronický podpis
Tato aplikace Vám umožní podepsat elektronický podpisem jeden či více dokumentů libovolného typu, a to jedním či více podpisovateli. Seznamte se, prosím, v nápovědě s doporučeným postupem podepisování dokumentů.
Jak vytvořit novou obálku s dokumenty určenými k podpisu
1. Zvolte položku menu Soubor/Nový
2. Vyberte jeden či více souborů, které chcete podepsat. Tyto soubory budou vloženy do obálky ve formátu XML.
3. Určete, kolik kol procesu podpisování proběhne (viz nápověda), kolik osob bude dokument podepisovat (není-li jejich počet určen, tuto položku nevyplňujte) a napište zprávu pro podepisující osoby
4. Vyberte certifikát, kterým podepíšete obálku s dokumenty a instrukcemi. Podpis obálky je určen k tomu, aby podepisující osoby měly jistotu, od koho tato obálka pochází, a že k nim byla doručena beze změny.
Více informací najdete v nápovědě.
© Multisignature | Aplikaci Multisignature vytvořil MathAn Praha, s.r.o. v rámci řešení projektu YA512006005 MIČR.
[15:57] Byla spuštěna aplikace

Kapitola 5. Zahájení procesu podepisování

Procesu podepisování obvykle předchází dohoda mezi podepisujícími stranami o stanovení nezávislého organizátora procesu podepisování. Tohoto nezávislého organizátora budeme označovat jako *koordinátora*. Této role se může ujmout také některá z podepisujících stran.

Koordinátor určí dokument (případně i více dokumentů), který se bude podepisovat. Tento dokument bude vložen do obálky a spolu s informací o jeho původním názvu. Dokument se do XML obálky vkládá v binární podobě.

Je-li podepisována smlouva, měla by obsahovat ujednání jednoznačně stanovující začátek její platnosti, aby nedošlo k situaci, že by některá ze stran přijala své závazky jednostranně. Účinnost tohoto protokolu (jak pro UVPD, tak pro UVPDD) závisí na poctivosti koordinátora a na spolehlivosti doručovacích mechanismů.

Dále koordinátor určí volitelné parametry procesu podepisování. Těmito parametry jsou počet podepisujících stran, textová zpráva pro podepisující strany a úroveň procesu podepisování, tj. kolik kol podepisování dokumentu proběhne.

Výsledný XML soubor koordinátor elektronicky podepíše, uloží a doručí podpisovatelům. Doručení podepisovaného souboru podpisovatelům aplikace neřeší. Je možné použít např. e-mail nebo jinou formu doručení.

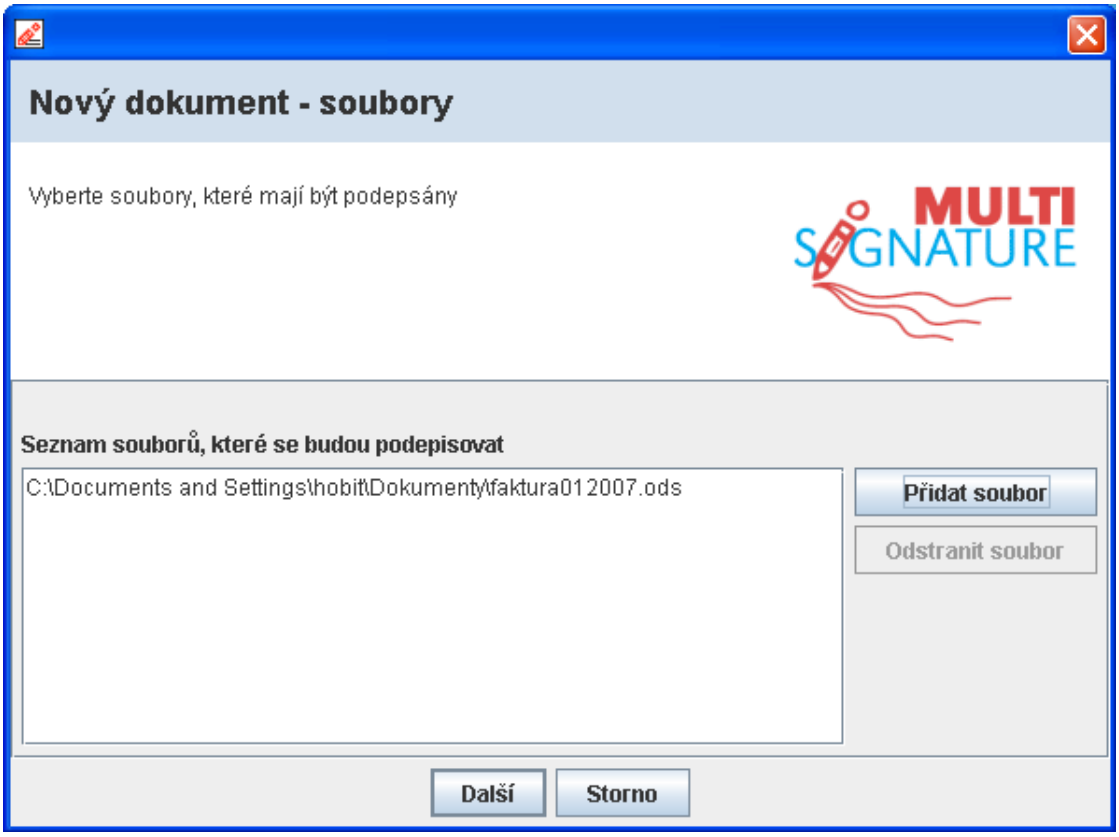
Podrobný postup vytvoření souboru je popsán zde (položky 1 - 6 provádí koordinátor):

1. Otevřete aplikaci Multisignature a pomocí položky menu Soubor → Nový založíte nový soubor, který bude podepisován.

2. V novém okně, které se Vám otevře, určete dokumenty, které mají být podepsány. Pomocí tlačítka Přidat soubor vyberte z adresářů ty soubory, které chcete společně podepisovat.

   Pokud některý z vybraných dokumentů chcete z výběru odstranit, označte jej myší a pomocí tlačítka Odstranit soubor jej odstraníte ze seznamu vybraných dokumentů.

   Stisknutím tlačítka OK potvrdíte výběr dokumentů určených k podepisování.



3. V nově zobrazeném okně zadejte instrukce pro řízení procesu podepisování.

   Aplikace nabízí čtyři úrovně procesu podepisování.

   - V první úrovni Základní podpisy získáte pouze sestavu dokumentů s připojenými dílčími podpisy podpisovatelů.

   - V druhé úrovni Uzavírací podpis získáte dokumenty s podpisy podpisovatelů a navíc s uzavíracím podpisem koordinátora, což vytváří tzv. uzavřený vícenásobně podepsaný dokument (UVPD). Koordinátor v něm svým podpisem stvrdí, že viděl dokument(y) s podpisy.

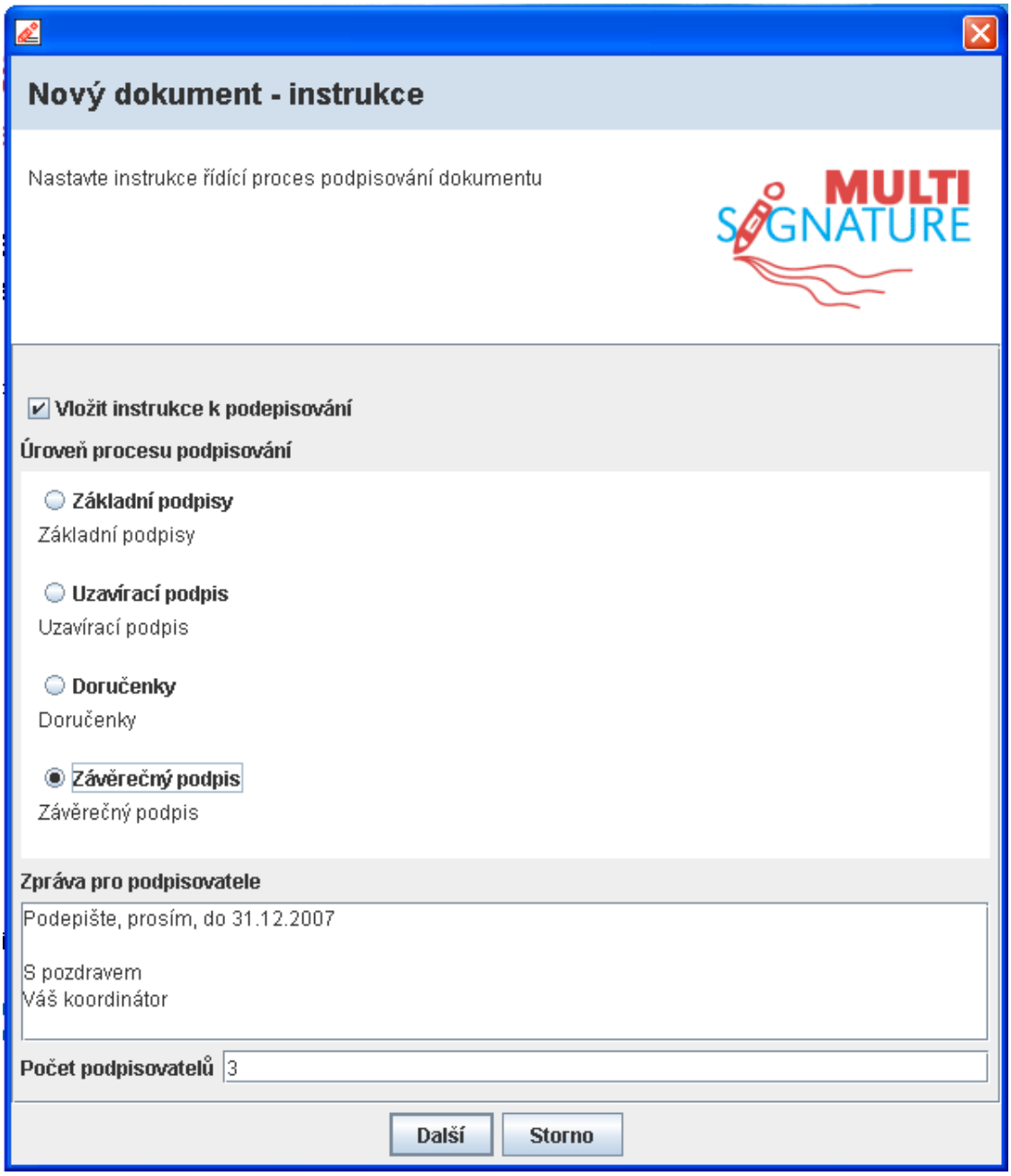
   - Ve třetí úrovni Doručenky získáte navíc od každého podpisovatele podepsanou doručenku potvrzující, že obdržel uzavřený vícenásobně podepsaný dokument.

   - Ve čtvrté úrovni Závěrečný podpis koordinátor k dokumentu s podpisy, uzavíracím podpisem a doručenkami připojí svůj podpis. Tento podpis potvrzuje, že viděl dokument(y) s podpisy, uzavíracím podpisem a doručenkami. Tím vznikne tzv. uzavřený vícenásobně podepsaný dokument s doručenkami (UVPDD). Tento dokument koordinátor rozešle všem podpisovatelům.

   Dále je možné napsat zprávu či pokyny pro podpisovatele.

   A v tomtéž okně lze také zadat počet podpisovatelů. Pokud žádné číslo nezadáte, program bude předpokládat, že počet podpisovatelů není předem znám (nebo určen).

   Tlačítkem OK potvrďte zadání instrukcí pro proces podepisování.



4. Po potvrzení instrukcí se objeví dialogové okno, které koordinátora vyzve k výběru jeho certifikátu, kterým podepíše výzvu k podepisování dokumentu. Je důležité, aby každý podpisovatel měl jistotu, že komunikuje s dohodnutým koordinátorem. K tomu slouží podpis pokynů koordinátorem.

   Koordinátor v levé části okna vybere úložiště certifikátů a v pravé části potom označí zvolený certifikát. (pro přístup do úložiště je třeba zadat heslo.) Tlačítkem OK se potvrdí volba certifikátu.

5. Po potvrzeni volby certifikátu se objeví nové okno "Uložit jako ...", které umožní uložit soubor s podpisem koordinátora pod novým názvem. Nový soubor se vytvoří s příponou *.mul*. Je to přípona pro soubory s elektronickými podpisy vzniklými v aplikaci Multisignature. Soubor lze uložit také pod původním jménem souboru, ale v tomto případě se původní soubor přepíše. Po uložení tlačítkem Uložit bude soubor s podpisem koordinátora uložen ve vybraném adresáři.

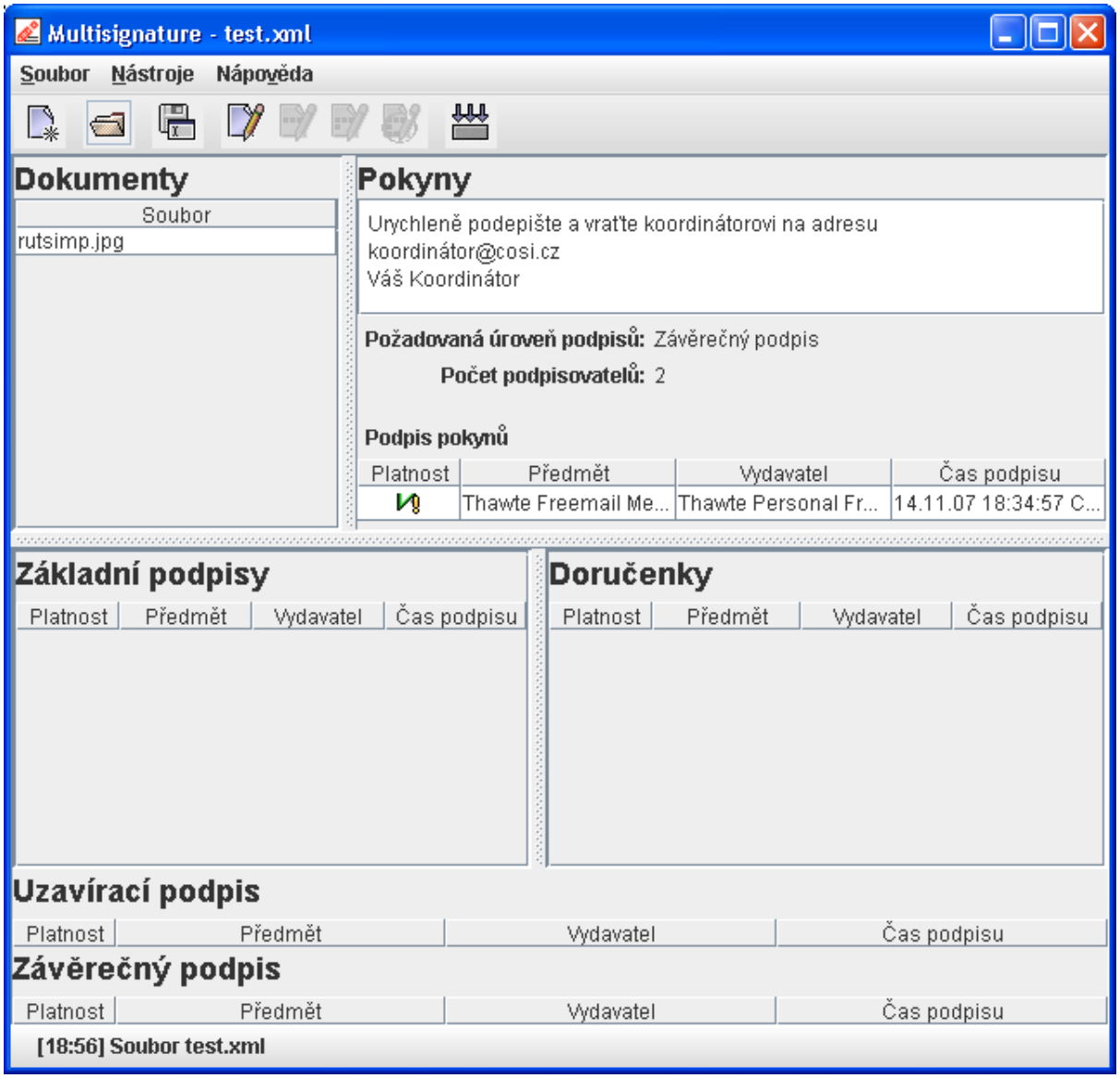
6. Takto vytvořený soubor s podepsanými pokyny rozešle koordinátor jednotlivým podpisovatelům. Způsob zaslání aplikace neřeší, koordinátor použije postup, který považuje za nejvhodnější. Nezmě-

nitelnost obsahu rozesílaného dokumentu je zaručena elektronickým podpisem koordinátora a tento podpis také zaručí podpisovatelům autentičnost zaslaného dokumentu.

7. Každý podpisovatel po otevření doručeného souboru v hlavním okně aplikace uvidí vlevo nahoře podepisované dokumenty a v pravém horním rámci je vidět podpis koordinátora. Kliknutím na řádek s názvem dokumentu lze dokument otevřít; kliknutím na řádek s podpisem se otevře okno popisující ověření certifikátu a parametry certifikátu - podrobnosti lze nalézt v oddílu Management klíčů a certifikátů.

Kapitola 6. Hlavní okno aplikace

Otevřením souboru s příponou **.mul** se soubor otevře v hlavním okně aplikace, kde je možné vidět názvy podepisovaných dokumentů, pokyny pro podepisující strany včetně podpisu koordinátora a dle zvolené úrovně podepisování rámce pro základní podpisy, uzavírací podpis, doručenky a závěrečný podpis.



6.1. Uživatelské akce hlavního okna aplikace

Kromě akcí přímo uvedených v menu aplikace a panelu nástrojů aplikace může uživatel provést následující akce:

- Dvojitým kliknutím na řádek s podepisovaným dokumentem se tento dokument otevře ve výchozí aplikaci systému určené k otevírání dokumentů tohoto typu určeného příponou názvu souboru
- Dvojitým kliknutím na řádek libovolného podpisu lze otevřít okno s ověřením a dalšími parametry podpisu.

Tabulka s podpisy obsahuje informace o platnosti podpisu, předmětu certifikátu, vydavateli certifikátu a čase podpisu. Čas podpisu je obsažen v každém podpisu jako jeho podepsaný atribut a vyjadřuje systémový čas počítače, na němž byl podpis vytvořen.

6.2. Význam ikon, které vyjadřují platnost podpisu

Podpis je zcela v pořádku, včetně ověření certifikační cesty a seznamů zneplatněných certifikátů (CRL)

Podpis a certifikační cesta jsou v pořádku, ověření seznamu zneplatněných certifikátů (CRL) zatím neproběhlo. Tuto akci musí uživatel iniciovat sám, a to na obrazovce podrobností o podpisu, která se zobrazí po dvojitém kliknutí na řádek s tímto podpisem

Podpis a certifikační cesta jsou v pořádku, ověření seznamu zneplatněných certifikátů proběhlo neúspěšně. Důvodem je buď, že certifikát byl zneplatněn, nebo špatná adresa umístění seznamu zneplatněných certifikátů (CRL)

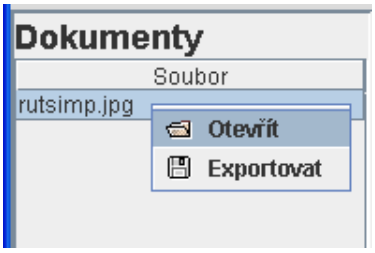
Podpis nelze považovat za platný. Buď byly podepsané dokumenty od okamžiku podpisu změněny nebo nelze ověřit certifikační cestu, např. její kořenová certifikační autorita nepatří mezi důvěryhodné certifikační autority. Pokud kořenová certifikační autorita nepatří mezi důvěryhodné certifikační autority a vy jí přesto důvěřujete, můžete její certifikát přidat do úložiště důvěryhodných certifikačních autorit.

Podpis nelze považovat za platný. Při jeho ověřování nastala nějaká neočekávaná chyba, která ověření platnosti podpisu zabránila.

Kapitola 7. Prohlédnutí podepisovaného dokumentu.

Podpisovatel si otevře XML obálku. Pro seznámení s dokumentem(ty), který je v obálce vložený, je možné tento dokument uložit jako samostatný soubor (použít pravé tlačítko myši a Exportovat). Tento soubor si pak lze prohlédnout v aplikaci odpovídající typu souboru.

Druhou variantou bude vložený dokument otevřít přímo z aplikace dvojitým kliknutím na řádek s názvem dokumentu nebo použitím pravého tlačítka myši a Otevřít. V tomto případě se k jeho otevření použije výchozí aplikace určená dle koncovky souboru.



Kapitola 8. Podepsání dokumentu jedním podpisovatelem - dílčí podpis

Bude-li otevřená XML obálka obsahovat již nějaké podpisy, aplikace je zobrazí včetně informace o jejich platnosti.

Pro podepsání souboru s příslušnými dokumenty a podpisem koordinátora musí podpisovatel nejprve vybrat úložiště certifikátů a certifikát, kterým chce podpis realizovat. Tímto certifikátem pak podpisovatel dokument podepíše. Takto vzniká tzv. dílčí podpis .

Úložiště certifikátu pro vytvoření dílčího podpisu lze vybrat přes Nástroje → Základní podpis nebo pomocí ikony 
v levé horní části obrazovky.

Podepsaný dokument podpisovatel doručí koordinátorovi.

Kapitola 9. Spojení dílčích podpisů

Po obdržení všech XML obálek s dílčími podpisy od jednotlivých podpisovatelů musí koordinátor všechny spojit do jednoho souboru.

Spojení souborů s dílčími podpisy lze provést přes Nástroje → Spojit podpisy nebo pomocí ikony  v levé horní části obrazovky. Po odkliknutí se otevře nové okno pro spojení podpisů. V něm koordinátor vybere typ spojovaných podpisů (v tomto případě Základní podpisy) a soubory obsahující dokument(y) a podpisy, které je třeba spojit do jednoho souboru.

Pomocí tlačítka Přidat vybere soubory, které chce spojit. Aplikace ověří, zda všechny vybrané soubory obsahují tentýž dokument. Pokud ano, vytvoří z nich soubor jediný, který bude obsahovat podepisovaný dokument i všechny jeho dílčí podpisy.

Obsahuje-li více ze spojovaných souborů tentýž podpis, zahrne se do výsledného souboru tento podpis právě jednou.

Při spojování podpisů aplikace postupuje stejně i v případě, že některé podpisy jsou neplatné - uživatele na to upozorní.

Kapitola 10. Uzavírací podpis a vytvoření uzavřeného vícenásobně podepsaného dokumentu

K podepsanému dokumentu lze připojit uzavírací podpis (nastavuje koordinátor při zahájení procesu podepisování). Vytváří ho koordinátor a stvrzuje tím všechny podpisy, kterými je soubor podepsán. Zároveň tím potvrdí, že viděl soubor, který obsahuje podepisované dokumenty a všechny podpisy.

Pro vytvoření uzavíracího podpisu lze použít v hlavní nabídce Nástroje → Uzavírací podpis nebo ikonu  v levé horní části obrazovky.

Spojením dílčích podpisů do jednoho souboru a doplněním uzavíracího podpisu vzniká uzavřený vícenásobně podepsaný dokument (UVPD).

Kapitola 11. Potvrzení doručenky

Pokud je požadováno podepisování doručenek (nastavuje koordinátor při zahájení procesu podepisování), obdrží každý podpisovatel žádost o potvrzení přijetí UVPD. Doručenka je potvrzením, že podpisovatel obdržel UVPD. Tato operace je realizována rovněž elektronickým podpisem.

Doručenku lze vytvořit přes Nástroje → Doručenka nebo pomocí ikony  v levé horní části obrazovky.

Doručenku podpisovatel vrátí koordinátorovi.

Kapitola 12. Vytvoření uzavřeného vícenásobně podepsaného dokumentu s doručenkami

Po obdržení doručenek od všech podpisovatelů musí koordinátor spojit jednotlivé soubory s doručenkami do jednoho souboru. Lze to provést přes Nástroje → Spojit podpisy nebo pomocí ikony  v levé horní části obrazovky. Po odkliknutí se otevře nové okno pro spojení podpisů. V něm koordinátor vybere typ spojovaných podpisů (v tomto případě Doručenky) a soubory obsahující dokument(y), podpisy, uzavírací podpis a doručenky, které je třeba spojit do jednoho souboru.

Pomocí tlačítka Přidat vybere soubory, které chce spojit. Aplikace ověří, zda všechny vybrané soubory obsahují tentýž dokument. Pokud ano, vytvoří z nich soubor jediný, který bude obsahovat podepisovaný dokument i všechny podpisy, uzavírací podpis a doručenky.

Obsahuje-li více ze spojovaných souborů tentýž podpis, zahrne se do výsledného souboru tento podpis právě jednou.

Při spojování podpisů aplikace postupuje stejně i v případě, že některé podpisy jsou neplatné - uživatele na to upozorní.

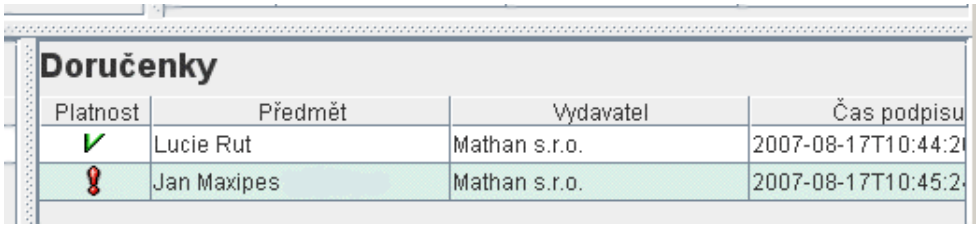
Po spojení všech doručenek koordinátor může soubor ještě uzavřít závěrečným podpisem (nastavuje koordinátor při zahájení podepisování). Lze to provést přes Nástroje → Závěrečný podpis nebo pomocí ikony  v levé horní části obrazovky.

Tak vznikne uzavřený vícenásobně podepsaný dokument s doručenkami (UVPDD).

Tento dokument pak koordinátor rozešle podpisovatelům.

Kapitola 13. Ověření platnosti podpisů

Aplikace vhodnou formou znázorní strukturu podpisů a podepisovaných dat ve vícenásobně podepsaném dokumentu nebo ve vícenásobně podepsaném dokumentu s doručenkami. Přitom ověří podpisy, které se v dokumentu vyskytují, a znázorní stav jejich ověření. Podpisy, které neprojdou ověřovací kontrolou aplikace, budou označeny červeným vykřičníkem (viz obrázek).



13.1. Význam ikon, které vyjadřují platnost podpisu

Podpis je zcela v pořádku, včetně ověření certifikační cesty a seznamů zneplatněných certifikátů (CRL)

Podpis a certifikační cesta jsou v pořádku, ověření seznamu zneplatněných certifikátů (CRL) zatím neproběhlo. Tuto akci musí uživatel iniciovat sám, a to na obrazovce podrobností o podpisu, která se zobrazí po dvojitém kliknutí na řádek s tímto podpisem

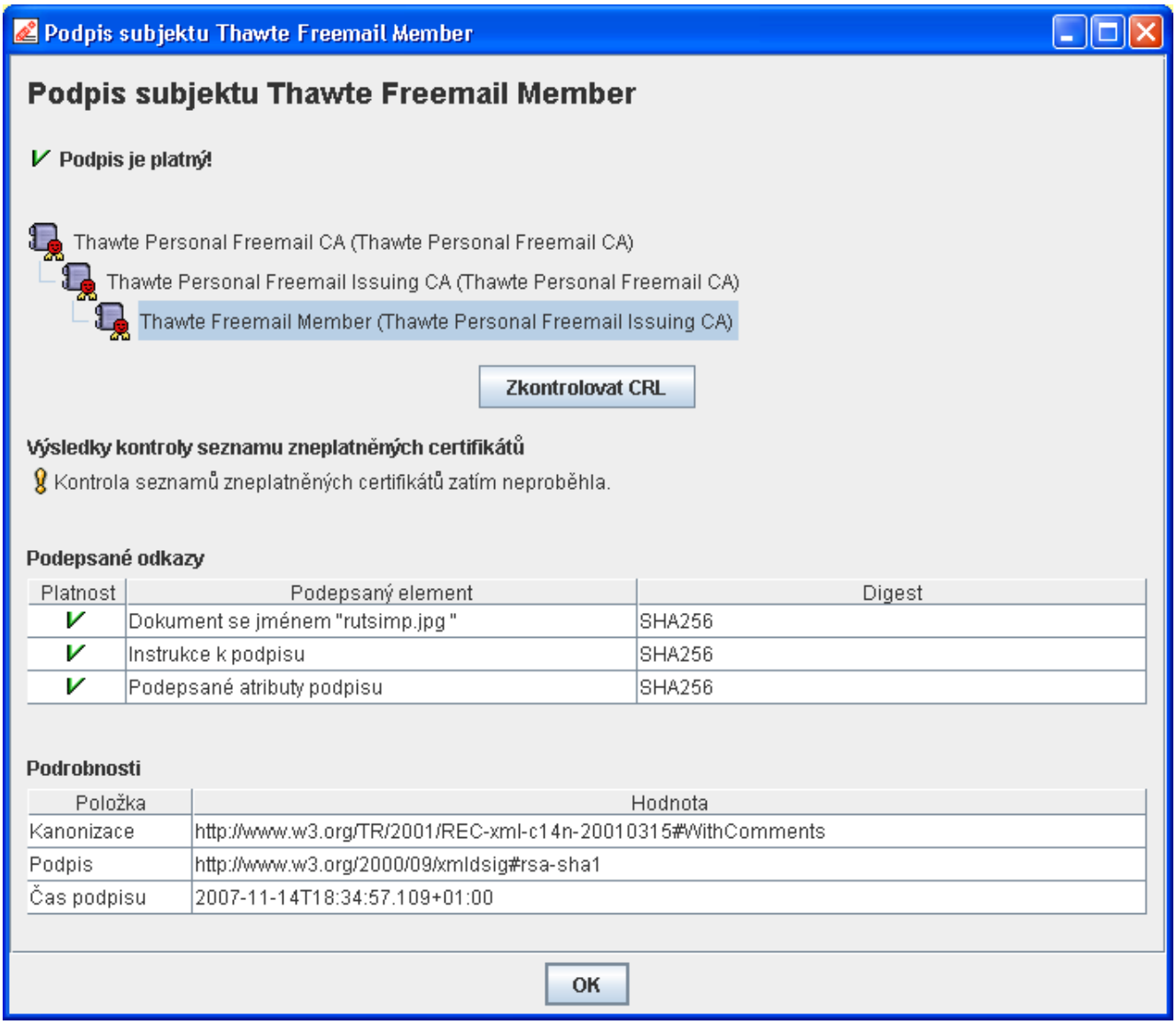
Podpis a certifikační cesta jsou v pořádku, ověření seznamu zneplatněných certifikátů proběhlo neúspěšně. Důvodem je buď, že certifikát byl zneplatněn, nebo špatná adresa umístění seznamu zneplatněných certifikátů (CRL)

Podpis nelze považovat za platný. Buď byly podepsané dokumenty od okamžiku podpisu změněny nebo nelze ověřit certifikační cestu, např. její kořenová certifikační autorita nepatří mezi důvěryhodné certifikační autority. Pokud kořenová certifikační autorita nepatří mezi důvěryhodné certifikační autority a vy jí přesto důvěřujete, můžete její certifikát přidat do úložiště důvěryhodných certifikačních autorit.

Podpis nelze považovat za platný. Při jeho ověřování nastala nějaká neočekávaná chyba, která ověření platnosti podpisu zabránila.

13.2. Podrobný popis ověření podpisu

Aplikace automaticky ověřuje vlastní podpis dokumentů a podepsaných atributů podpisu. Dále automaticky ověřuje, zda certifikační cesta obsažená v podpisu končí u důvěryhodné autority, tj. autority, jejíž certifikát je obsažen v úložišti certifikátů certifikačních autorit nakonfigurovaném s pomocí **Správce certifikátů** aplikace Multisignature. Podrobné informace o digitálním podpisu a jeho stavu platnosti se zobrazí po dvojitém kliknutí na řádek s tímto podpisem.



Okno s podrobnymi nformacemi o podpisu obsahuje nejprve údaj o platnosti samotného podpisu. Pod tímto údajem je zobrazena certifikační cesta obsažená v podpisu. Dále je zobrazena tabulka s podrobnými informacemi o tom, jaké údaje jsou podepsány a tabulka s informacemi o použitých algoritmech podpisu a čase podpisu. Nyní tyto údaje popíšeme podrobněji.

13.2.1. Vlastní podpis a jeho ověření

Stav platnosti podpisu je zobrazen hned pod nadpisem okna s podrobnými informacemi o podpisu. Při vytváření podpisu se nejprve spočítají digesty (otisky) z obsahu všech podepsaných odkazů a vloží do XML elementu podpisu. Pak se všechny tyto otisky dohromady podepíší. Podpis může být neplatný z více různých důvodů.

- Podepsaný dokument byl změněn!
- Podpis nelze ověřit certifikátem v něm obsaženým!
- Není k dispozici certifikát k ověření podpisu!
- Certifikát nebyl v době podpisu platný!
- Certifikáty, které podpis obsahuje, neodpovídají podepsaným otiskům certifikátů!
- Některé dokumenty nejsou podepsány!
- Podpis neobsahuje podepsaný atribut s otisky použitých certifikátů!
- Vlastnosti podpisu, které by měly být podepsány, podepsány nejsou!
- Nejsou podepsány základní podpisy!
- Není podepsán uzavírací podpis!
- Nejsou podepsány doručenky!
- Nastala chyba při pokusu o kontrolu podepsaných odkazů!
- Je podepsáno více odkazů, než by mělo být!

13.2.2. Certifikační cesta a její ověření

Certifikát, kterým je vytvořen podpis, je podepsán nějakou certifikační autoritou. K ověření tohoto podpisu je potřeba mít k dispozici příslušný certifikát této autority. Certifikát certifikační autority může být podepsaný jinou certifikační autoritou nebo tou samou certifikační autoritou. V tom druhém případu hovoříme o kořenovém certifikátu. Posloupnost všech těchto certifikátů od certifikátu uživatele až ke kořenovému certifikátu se nazývá certifikační cesta nebo také řetěz certifikátů.

Při ověření certifikační cesty se ověřuje, zda jsou podpisy certifikátů z této cesty platné a zda kořenový certifikát patří důvěryhodné certifikační autoritě, tj. autoritě, které věříme, že nedá certifikát potvrzující nějaké údaje (třeba identitu) špatné osobě.

Nelze-li certifikační cestu ověřit, je informace o chybě zobrazena nad touto certifikační cestou.

13.2.3. Ověření seznamu zneplatněných certifikátů (CRL)

Ověření, zda některý z certifikátů certifikační cesty nebyl zneplatněn, neprobíhá automaticky, neboť tato akce vyžaduje přístup k internetu a může být časově náročná. Tato akce se iniciuje z obrazovky podrobností o digitálním podpisu, která obsahuje tlačítko s nápisem **Zkontrolovat CRL** a pod ním informace o výsledku kontroly seznamu zneplatněných certifikátů.

Při ověřování seznamu zneplatněných certifikátů se adresa obsahující potřebný seznam získá automaticky z digitálního certifikátu. Pokud ji certifikát neobsahuje, musí ji uživatel vyplnit do dialogového okna, které se otevře. Správnou adresu lze získat na stránkách certifikační autority, která certifikát podepsala.

13.2.4. Tabulka "Podepsané odkazy"

Tato tabulka vypisuje všechny podepsané odkazy podpisu. Položka popis ukazuje, zda je odkaz platný, tj. obsah odkazu je stejný jako v době podpisu. Každý podpis by měl dle svého typu obsahovat následující podepsané odkazy:

Podpis instrukcí	Podpisy všech podepisovaných dokumentů Instrukce k podpisu Podepsané atributy podpisu
Základní podpis	Podpisy všech podepisovaných dokumentů Podepsané atributy podpisu
Uzavírací podpis	Seznam základních podpisů Podepsané atributy podpisu
Podpis jako doručenka	Uzavíracího podpisu Podepsané atributy podpisu
Závěrečný podpis	Seznam doručenek Podepsané atributy podpisu

13.2.5. Tabulka "Podrobnosti"

Tato tabulka obsahuje algoritmy použité při tvorbě podpisu a cas podpisu:

- **Kanonizace** - algoritmus, kterým se podepisovaná část XML převede do kanonické podoby, provádí pouze "kosmetické" úpravy struktury a obsahu upravované části XML dokumentu
- **Podpis** - algoritmus podpisu, obsahuje definici metody výpočtu digestu (otisku) podpisovaných dat a algoritmus zašifrování tohoto digestu
- **Čas podpisu** - lokální čas počítače, na němž byl podpis vytvořen

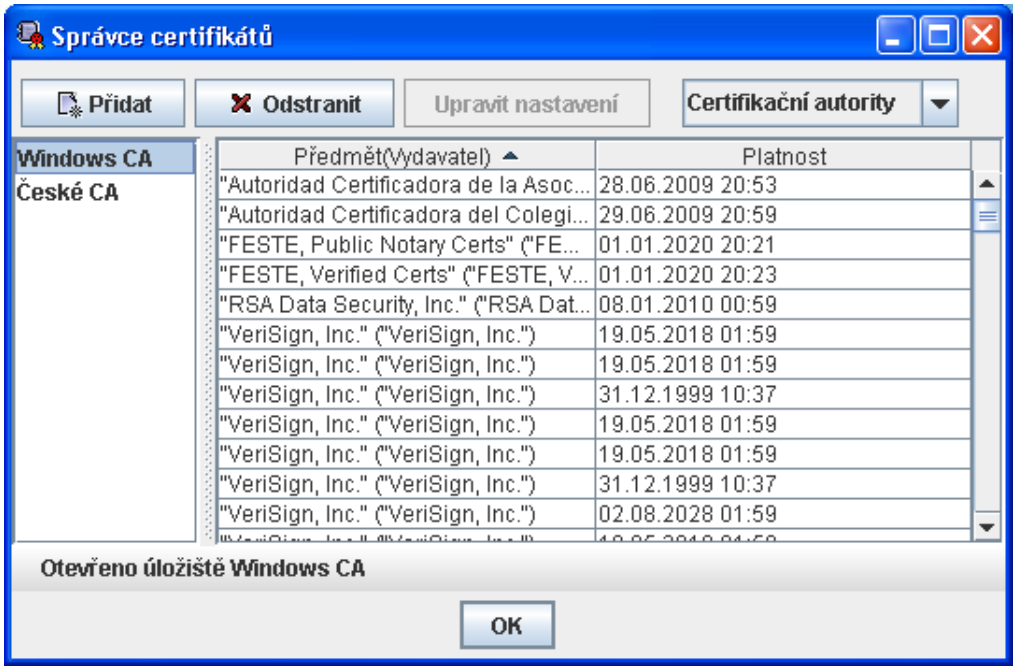
Kapitola 14. Management klíčů a certifikátů

Aplikace nevytváří vlastní úložiště klíčů a certifikátů, ale používá úložiště, která jsou k dispozici. Na operačním systému Windows bude primárně použito standardní úložiště poskytované operačním systémem a zpřístupněné přes MS CryptoAPI.

Jako další možnost lze použít úložiště organizované prostředím Java v souborech typu JKS (Java KeyStore) nebo PFX či P12 (standardní formát PKCS#12).

Další možností je podpora úložiště klíčů NSS (Mozilla/Firefox) a konečně přístup k hardwarovým bezpečnostním tokenům prostřednictvím rozhraní PKCS#11.

Aplikace obsahuje manažera úložišť certifikátů, kde je možné používání těchto úložišť nastavit. Do úložiště certifikátů se dostanete z hlavní nabídky přes Nástroje → Správce certifikátů. V okně, které se Vám otevře, můžete pomocí tlačítka Přidat nastavit Vaše úložiště certifikátů. Zadáte jméno úložiště, vyberete typ a pomocí tlačítka Další postoupíte dále. V následujícím okně zadáte cestu k souboru, který obsahuje úložiště certifikátů. Po potvrzení tlačítkem OK se úložiště zobrazí v seznamu v okně Správce certifikátů (viz obrázek).



Kapitola 15. Příklady

15.1. Podpis smlouvy dvěma nebo více rovnocennými stranami

1. Strany nejprve určí koordinátora procesu podepisování. Tento koordinátor může (ale nemusí) být jednou z podepisujících stran. Je-li koordinátor jednou ze stran, měl by své role koordinátora a podpisovatele důsledně oddělovat.

2. Koordinátor vytvoří XML obálku s podepisovaným dokumentem a žádostí o dílčí podpis a rozešle ji podpisovatelům.

3. Každý podpisovatel obdrženou XML obálku otevře, přidá svůj dílčí podpis a vrátí ji koordinátorovi.

4. Koordinátor spojí podpisy všech podpisovatelů do jednoho dokumentu a zkontroluje jejich platnost. Pokud jsou všechny podpisy platné, připojí svůj uzavírací podpis. Tím vznikne UVPD.

Nejsou-li požadovány doručenky, pak koordinátor UVPD prostě jen rozešle podepisujícím stranám.

V případě, že strany chtějí mít zaručeno, že žádná z nich nepřijme závazky smlouvy jednostranně, použijí následující protokol, který zajistí potvrzené doručení UVPD. Jde v zásadě o zopakování postupu podpisu základního dokumentu:

1. Koordinátor do UVPD doplní žádost o potvrzení doručení a rozešle jej podpisovatelům.

2. Každý z podpisovatelů ověří platnost podpisů v UVPD. Pokud jsou všechny platné, podpisovatel podepíše UVPD jakožto „doručenku“ a výsledek vrátí koordinátorovi. Tímto podpisem potvrzuje obdržení UVPD, nikoli souhlas s jeho obsahem. Nejsou-li všechny podpisy v UVPD platné, doporučuje se doručenku nepodepsat.

3. Koordinátor obdržené a podepsané dokumenty s doručenkami spojí. Výslednou obálku s dokumentem, všemi podpisy a se všemi doručenkami podepíše svým závěrečným podpisem. Tím vznikne UVPDD, který koordinátor rozešle všem podepisujícím stranám.

Podepisovaná smlouva by měla obsahovat jednoznačné ujednání o začátku platnosti. Je dobré stanovit, že smlouva nabývá platnosti okamžikem potvrzení doručenek všemi stranami. Protože není zaručeno, že u všech stran to bude přibližně jeden okamžik, je vhodné počátek účinnosti smlouvy nevázat na počátek její platnosti.

15.2. Podpis petice

1. Organizátor petice vytvoří XML obálku, do které se budou vkládat podpisy. V tomto případě může být výhodné podepisovanou petici nevkládat přímo do obálky, ale vystavit ji na webové stránce a do XML obálky vložit pouze odkaz na tuto webovou stránku.

2. XML obálku organizátor petice buď rozešle přímo zájemcům o podpis, nebo ji vystaví na internetu, odkud si ji mohou všichni podpisovatelé stáhnout.

3. Podpisovatel petice podepíše XML obálku a zašle ji organizátorovi. Je možná i varianta, že do jedné XML obálky přidá svůj podpis více osob a organizátorovi se odešle tedy s více než jedním podpisem.

4. Organizátor petice spojí všechny obdržené podepsané obálky do jediného souboru.

Kapitola 16. Schéma procesu podepisování

Koordinátor	Podpisovatel A	Podpisovatel B
1. Vytvoří obálku s podepisovaným dokumentem a pokyny.	-	-
2. Podepíše obálku a pošle podpisovatelům (A, B).	-	-
-	3A. Zkontroluje dokument a identitu koordinátora.	3B. Zkontroluje dokument a identitu koordinátora.
-	4A. Podepíše – dílčí podpis a pošle zpět koordinátorovi.	4B. Podepíše – dílčí podpis a pošle zpět koordinátorovi.
5. Zkontroluje vrácené obálky, jejich podpisy a identity podpisovatelů.	-	-
6. Spojí a podepíše uzavírací podpis. Zde může proces podepisování ukončit, nebo pošle opět podpisovatelům.	-	-
-	7A. Zkontroluje dokumenty, dílčí podpisy, uzavírací podpis a identitu koordinátora.	7B. Zkontroluje dokumenty, dílčí podpisy, uzavírací podpis a identitu koordinátora.
-	8A. Podepíše – doručenka a pošle zpět koordinátorovi.	8B. Podepíše – doručenka a pošle zpět koordinátorovi.
9. Zkontroluje vrácené obálky, jejich podpisy, uzavírací podpis, identity podpisovatelů a doručenky.	-	-
10. Spojí doručenky, připojí svůj závěrečný podpis a pošle podpisovatelům.	-	-
Archivuje.	Archivuje.	Archivuje.

Rejstřík